Local Transition Functions of Quantum Turing Machines

AUTHOR(S):

Ozawa, Masanao; Nishimura, Harumichi

CITATION:

Ozawa, Masanao ...[et al]. Local Transition Functions of Quantum Turing Machines. 数理解析研究所講究録 1999, 1100: 168-181

ISSUE DATE:

1999-06

URL:

http://hdl.handle.net/2433/63151

数理解析研究所講究録
1100巻 1999年 168-181

Local Transition Functions of Quantum Turing Machines (量子 Turing 機械の局所遷移関数)

MASANAO OZAWA (小澤 正直), HARUMICHI NISHIMURA (西村 治道)
School of Informatics and Sciences and Graduate School of Human Informatics
Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan

Abstract

Foundations of the notion of quantum Turing machines are investigated. According to Deutsch's formulation, the time evolution of a quantum Turing machine is to be determined by the local transition function. In this paper, the local transition functions are characterized for fully general quantum Turing machines, including multi-tape quantum Turing machines, extending an earlier attempt due to Bernstein and Vazirani.

1. Introduction

Feynman [1] pointed out that a Turing machine cannot simulate a quantum mechanical process efficiently and suggested that a computing machine based on quantum mechanics might be more powerful than Turing machines. Deutsch introduced quantum Turing machines [2] and quantum circuits [3] for establishing the notion of quantum algorithm exploiting "quantum parallelism". A different approach to quantum Turing machines was taken earlier by Benioff [4] based on the Hamiltonian description of Turing machines. Bernstein and Vazirani [5] instituted quantum complexity theory based on quantum Turing machines and constructed an efficient universal quantum Turing machine. Yao [6] showed that a computation by a quantum Turing machine can be simulated efficiently by a quantum circuit. Deutsch's idea of quantum parallelism was realized strikingly by Shor [7], who found efficient quantum algorithms for the factoring problem and the discrete logarithm problem, for which no efficient algorithms have been found for classical computing machines.

In this paper, foundations of the concept of quantum Turing machines are examined. In Deutsch's formulation [2], a quantum Turing machine is defined to be a quantum system consisting of a processor, a moving head, and a tape, obeying a unitary time evolution determined by local interactions between its components, and allowing to be in a superposition of computational configurations. Deutsch [2] pointed out that the global transition function between computational configurations should be determined by a local transition function which depends only on local configurations. Recently, Bernstein and Vazirani [8] found a

simple characterization of the local transition functions for the restricted class of quantum Turing machines in which the head must move either to the right or to the left at each step. Since the above characterization constitutes an alternative definition of quantum Turing machines more tractable in the field of theoretical computer science, it is an interesting problem to find a general characterization valid even when the head is not required to move or more generally when the machines has more than one tape. The purpose of this paper is to solve this problem, while for this and foundational purposes we also provide a completely formal treatment of the theory of quantum Turing machines.

2. Quantum Turing Machine as a physical system

A *quantum Turing machine* $\mathcal{Q}$ is a quantum system consisting of a *processor*, a bilateral infinite *tape*, and a *head* to read and write a symbol on the tape. Its configuration is determined by the *processor configuration* q from a finite set Q of symbols, the *tape configuration* T represented by an infinite string from a finite set Σ of symbols, and the discretized *head position* ξ taking values in the set $\mathbf{Z}$ of integers. The tape consists of *cells* numbered by the integers. The head position $\xi \in \mathbf{Z}$ stands for the place of the cell numbered by ξ. We assume that Σ contains the symbol B representing the blank cell in the tape. For any integer m the symbol at the cell m on the tape is denoted by $T(m)$. We assume that the possible tape configurations are such that $T(m) = B$ except for finitely many cells m. The set of all the possible tape configurations is denoted by $\Sigma^{\#}$. The set $\Sigma^{\#}$ is a countable set. Thus, any configuration C of $\mathcal{Q}$ is represented by a triple $C = (q, T, \xi)$ in the configuration space $\mathcal{C}(Q, \Sigma) = Q \times \Sigma^{\#} \times \mathbf{Z}$. The quantum state of $\mathcal{Q}$ is represented by a unit vector in the Hilbert space $\mathcal{H}(Q, \Sigma)$ generated by the configuration space $\mathcal{C}(Q, \Sigma)$. The complete orthonormal basis canonically in one-to-one correspondence with the configuration space is called the *computational basis*. Thus, the computational basis is represented by $|C\rangle = |q, T, \xi\rangle$ for any configuration $C = (q, T, \xi) \in \mathcal{C}(Q, \Sigma)$.

In order to define the observables quantizing the configurations, we assume the numbering of the sets Q and Σ such that $Q = \{q_0, \ldots, q_{|Q|-1}\}$ and $\Sigma = \{\sigma_0, \ldots, \sigma_{|\Sigma|-1}\}$, where we denote by $|X|$ the number of the elements of a set X.

We define observables $\hat{q}$, $\hat{T}(m)$ for $m \in \mathbf{Z}$, and $\hat{\xi}$ as follows.

$$\hat{q} = \sum_{n=0}^{|Q|-1} n|q_n\rangle\langle q_n|, \quad \hat{T}(m) = \sum_{n=0}^{|\Sigma|-1} n|\sigma_n\rangle\langle\sigma_n|, \quad \hat{\xi} = \sum_{\xi\in\mathbf{Z}} \xi|\xi\rangle\langle\xi|.$$

The computation begins at $t = 0$ and proceeds in steps of a fixed unit duration τ. Since the position of the head is discretized, the wave function $|\psi(t)\rangle$ may not stay within $\mathcal{H}(Q, \Sigma)$ at any time t other than integer multiples of τ. We assume therefore that the time t is discretized to be an integer multiple of τ. We also take the normalized unit of time in which the time t takes values in $\mathbf{Z}$. The dynamics of $\mathcal{Q}$ are described by a unitary operator U on $\mathcal{H}(Q, \Sigma)$ which specifies the evolution of any quantum state $|\psi(t)\rangle$ during a single

computational step so that we have

$$U^\dagger U = UU^\dagger = I, \quad |\psi(t)\rangle = U^t|\psi(0)\rangle \tag{1}$$

for all positive integer t.

3. Local transition functions

Deutsch [2] required that the quantum Turing machine operates finitely, i.e., (i) only a finite system is in motion during any one step, (ii) the motion depends only on the quantum state of a local subsystem, and (iii) the rule that specifies the motion can be given finitely in the mathematical sense. To satisfy the above requirements, the matrix elements of U are required to take the following form[1]:

$$\begin{aligned}
&\langle q', T', \xi' | U | q, T, \xi \rangle \\
&\quad = [\boldsymbol{\delta}_{\xi'}^{\xi+1} \delta(q, T(\xi), q', T'(\xi), 1) + \boldsymbol{\delta}_{\xi'}^{\xi} \delta(q, T(\xi), q', T'(\xi), 0) \\
&\qquad + \boldsymbol{\delta}_{\xi'}^{\xi-1} \delta(q, T(\xi), q', T'(\xi), -1)] \prod_{m \neq \xi} \boldsymbol{\delta}_{T(m)}^{T'(m)}
\end{aligned} \tag{2}$$

for any configurations (q, T, ξ) and (q', T', ξ'). The continued product on the right ensures that the tape is changed only at the head position ξ at the beginning of each computational step. The terms $\boldsymbol{\delta}_{\xi'}^{\xi\pm1}$, $\boldsymbol{\delta}_{\xi'}^{\xi}$, where $\boldsymbol{\delta}$ denotes the Kronecker delta, ensure that during each step the head position cannot change by more than one unit. The function $\delta(q, T(\xi), q', T'(\xi), d)$, where $q, q' \in Q$, $T(\xi), T'(\xi) \in \Sigma$, and $d \in [-1, 1]_{\mathbf{Z}}$, represents a dynamical motion depending only on the local observables $\hat{q}$ and $\hat{T}(\xi)$. Here, for $n < m$ we denote by $[n, m]_{\mathbf{Z}}$ the interval $\{n, \ldots, m\}$ in the set of integers. We call δ the *local transition function* of the quantum Turing machine $\mathcal{Q}$.

The local transition function δ can be arbitrarily given except for the requirement Eq. (1) that U be unitary. Each choice defines a different quantum Turing machine $\mathcal{Q}[\delta]$ with the same configuration space $\mathcal{C}(Q, \Sigma)$. Thus, if we have an intrinsic characterization of the local transition function δ, quantum Turing machines can be defined formally without referring to the unitary operator U as a primitive notion.

From Eq. (2), the time evolution operator U is determined conversely from the local transition function δ by

$$U|q, T, \xi\rangle = \sum_{p, \tau, d} \delta(q, T(\xi), p, \tau, d) |p, T_\xi^\tau, \xi + d\rangle. \tag{3}$$

for any configuration (q, T, ξ), where T_ξ^τ is the tape configuration defined by

$$T_\xi^\tau(m) = \begin{cases} \tau & \text{if } m = \xi, \\ T(m) & \text{if } m \neq \xi. \end{cases} \tag{4}$$

[1]This condition is a natural extension of Deutsch's condition [2] to the case where the head is not required to move.

It follows that the relation $\delta(q,\sigma,q',\tau,d)=c$ can be interpreted as the following operation of $\mathcal{Q}$: if the processor is in the configuration q and if the head reads the symbol σ, then it follows with the amplitude c that the processor configuration turns to q', the head writes the symbol τ, and that the head moves one cell to the right if $d=1$, to the left if $d=-1$, or does not move if $d=0$.

Now we can formulate the characterization problem of local transition functions of quantum Turing machines: *Let δ be a complex-valued function on $Q\times\Sigma\times Q\times\Sigma\times[-1,1]_{\mathbf{Z}}$ and let U be the operator on $\mathcal{H}(Q,\Sigma)$ defined by Eq. (3). Then, what conditions ensure that the operator U is unitary?*

This problem is answered by the following statement: *The operator U is unitary if and only if δ satisfies the following conditions.*

(a) *For any $(q,\sigma)\in Q\times\Sigma$,*

$$\sum_{p,\tau,d}|\delta(q,\sigma,p,\tau,d)|^2=1.$$

(b) *For any $(q,\sigma),(q',\sigma')\in Q\times\Sigma$ with $(q,\sigma)\neq(q',\sigma')$,*

$$\sum_{p,\tau,d}\delta(q',\sigma',p,\tau,d)^*\delta(q,\sigma,p,\tau,d)=0.$$

(c) *For any $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$, we have*

$$\sum_{p\in Q,d=0,1}\delta(q',\sigma',p,\tau',d-1)^*\delta(q,\sigma,p,\tau,d)=0.$$

(d) *For any $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$, we have*

$$\sum_{p\in Q}\delta(q',\sigma',p,\tau',-1)^*\delta(q,\sigma,p,\tau,1)=0.$$

The proof will be given in the next section. If it is assumed that the head must move either to the right or to the left at each step, the condition (c) is automatically satisfied. In this case, the above statement is reduced to the result due to Bernstein and Vazirani [5]. In section 5, we will also characterize the local transition functions of two-tape quantum Turing machines and the generalization to multi-tape quantum Turing machines is suggested.

In order to maintain the Church-Turing thesis, we need to require that the unitary operator U is constructive, or that the range of the local transition function δ is in the computable complex numbers. From the complexity theoretical point of view, we need also to require that the matrix elements of U are polynomially computable complex numbers, or that the range of the transition function δ is in the polynomially computable complex numbers. Computational complexity of quantum Turing machines defined by the above conditions will be discussed in the forthcoming paper [9].

4. Quantum Turing machine as a mathematical structure

In order to formulate the notion of a quantum Turing machine as a formal mathematical structure rather than a well-described physical system, we shall introduce the following mathematical definitions. A *Turing frame* is a pair (Q, Σ) of a finite set Q and a finite set Σ with a specific element denoted by B. In what follows, let (Q, Σ) be a Turing frame. Let $\Sigma^{\#}$ be the set of functions T from the set $\mathbf{Z}$ of integers to Σ such that $T(m) = B$ except for finitely many $m \in \mathbf{Z}$. The *configuration space* of (Q, Σ) is the product set $\mathcal{C}(Q, \Sigma) = Q \times \Sigma^{\#} \times \mathbf{Z}$. The *quantum state space* of (Q, Σ) is the Hilbert space $\mathcal{H}(Q, \Sigma)$ spanned by $\mathcal{C}(Q, \Sigma)$ with the canonical basis $\{|C\rangle | \ C \in \mathcal{C}(Q, \Sigma)\}$ called the *computational basis*. A *local transition function* for (Q, Σ) is a function from $Q \times \Sigma \times Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$ into the complex number field $\mathbf{C}$.

In what follows, let δ be a local transition function for (Q, Σ). The *evolution operator* of δ is a linear operator M_δ on $\mathcal{H}(Q, \Sigma)$ such that

$$M_\delta |q, T, \xi\rangle = \sum_{p,\tau,d} \delta(q, T(\xi), p, \tau, d) |p, T^\tau_\xi, \xi + d\rangle \tag{5}$$

for all $(q, T, \xi) \in \mathcal{C}(Q, \Sigma)$; the summation $\sum_{p,\tau,d}$ is taken over all $(p, \tau, d) \in Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$ above and in the rest of this section unless stated otherwise. The domain of M_δ is defined to be the set of all $|\psi\rangle \in \mathcal{H}(Q, \Sigma)$ such that

$$\sum_{C \in \mathcal{C}(Q,\Sigma)} |\langle C|\psi\rangle|^2 \| M_\delta |C\rangle \|^2 < \infty. \tag{6}$$

For any $(p, \tau, d) \in Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$, denote by $\mathcal{C}(p, \tau, d)$ the set of configurations $(p, T, \xi) \in \mathcal{C}(Q, \Sigma)$ such that $T(\xi - d) = \tau$. Let $(p, \tau, d) \in Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$. We define the transformation $\alpha(p, \tau, d)$ from $\mathcal{C}(Q, \Sigma)$ to $\mathcal{C}(p, \tau, d)$ by

$$\alpha(p, \tau, d)(q, T, \xi) = (p, T^\tau_\xi, \xi + d)$$

for all $(q, T, \xi) \in \mathcal{C}(Q, \Sigma)$. It is easy to see that $\alpha(p, \tau, d)$ represents the operation such that the processor configuration turns to p, the head writes the symbol τ, and then moves with $|d|$ step to the direction d. We define the transformation $\beta(p, \tau, d)$ from $\mathcal{C}(Q, \Sigma)$ to $\mathcal{C}(p, \tau, 0)$ by

$$\beta(p, \tau, d)(q, T, \xi) = (p, T^\tau_{\xi - d}, \xi - d)$$

for any $(q, T, \xi) \in \mathcal{C}(Q, \Sigma)$. It is easy to see that $\beta(p, \tau, d)$ represents the operation such that the processor configuration turns to p, the head moves with $|d|$ step to the direction $-d$ and then writes the symbol τ. The following proposition can be checked by straightforward verifications.

Proposition 1. (i) *Let* $d \in [-1, 1]_{\mathbf{Z}}$. *If* $(q, \sigma) \neq (q', \sigma') \in Q \times \Sigma$ *then* $\mathcal{C}(q, \sigma, d) \cap \mathcal{C}(q', \sigma', d) = \emptyset$ *and*

$$\mathcal{C}(Q, \Sigma) = \bigcup_{(q,\sigma) \in Q \times \Sigma} \mathcal{C}(q, \sigma, d).$$

(ii) *Let* $(q,\sigma,p,\tau,d) \in Q \times \Sigma \times Q \times \Sigma \times [-1,1]_{\mathbf{Z}}$. *We have*

$$\beta(q,\sigma,d)\alpha(p,\tau,d)C = C$$

for all $C \in \mathcal{C}(q,\sigma,0)$ *and*

$$\alpha(p,\tau,d)\beta(q,\sigma,d)C' = C'$$

for all $C' \in \mathcal{C}(p,\tau,d)$.

(iii) *The mapping* $\alpha(p,\tau,d)$ *restricted to* $\mathcal{C}(q,\sigma,0)$ *has the inverse mapping* $\beta(q,\sigma,d)$ *restricted to* $\mathcal{C}(p,\tau,d)$, *i.e.,*

$$\mathcal{C}(q,\sigma,0) \underset{\beta(q,\sigma,d)}{\overset{\alpha(p,\tau,d)}{\rightleftarrows}} \mathcal{C}(p,\tau,d).$$

A configuration (q,T,ξ) is said to *precede* a configuration (q',T',ξ'), in symbols $(q,T,\xi) \prec (q',T',\xi')$, if $T'(m) = T(m)$ for all $m \neq \xi$ and $|\xi' - \xi| \leq 1$. The following proposition can be checked easily.

Proposition 2. *For any* $C, C' \in \mathcal{C}(Q,\Sigma)$, *the following conditions are equivalent.*
(i) $C \prec C'$.
(ii) *There is some* $(p,\tau,d) \in Q \times \Sigma \times [-1,1]_{\mathbf{Z}}$ *such that* $C' = \alpha(p,\tau,d)C$.
(iii) *There is some* $(q,\sigma,d) \in Q \times \Sigma \times [-1,1]_{\mathbf{Z}}$ *such that* $C = \beta(q,\sigma,d)C'$.

Proof. Let $C = (q,T,\xi)$ and $C' = (q',T',\xi')$.
(i)⇒(ii): If (i) holds, we have $C' = \alpha(q',T'(\xi),\xi' - \xi)C$ so that (ii) holds.
(ii)⇒(iii): Suppose that (ii) holds. Since $C \in \mathcal{C}(q,T(\xi),0)$, by Proposition 1 (ii) we have

$$\beta(q,T(\xi),d)C' = \beta(q,T(\xi),d)\alpha(p,\tau,d)C = C.$$

(iii)⇒(i): If (iii) holds, we have $C = (p, T'^{\sigma}_{\xi'-d}, \xi' - d)$ and hence $\xi' - \xi = d$ and $T(m) = T'^{\sigma}_{\xi'-d}(m) = T'(m)$ for $m \neq \xi' - d = \xi$ so that (i) holds. *QED*

Let (q,T,ξ), $(q',T',\xi') \in \mathcal{C}(Q,\Sigma)$. The following formula can be verified from Eq. (5) by straightforward calculation.

$$\langle q',T',\xi'|M_\delta|q,T,\xi\rangle = \begin{cases} \delta(q,T(\xi),q',T'(\xi),\xi'-\xi) & \text{if } (q,T,\xi) \prec (q',T',\xi'), \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

A configuration (q,T,ξ) is said to be *locally like* a configuration (q',T',ξ') if $q = q'$ and $T(\xi + d) = T'(\xi + d)$ for all $d \in [-1,1]_{\mathbf{Z}}$.

Lemma 3. *For any* $C_1, C_2 \in \mathcal{C}(Q,\Sigma)$, *if they are locally like each other, we have*

$$\langle C_1|M_\delta M_\delta^\dagger|C_1\rangle = \langle C_2|M_\delta M_\delta^\dagger|C_2\rangle.$$

Proof. Let $\tau_{-1}, \tau_0, \tau_1 \in \Sigma$. Suppose that a configuration $C' = (p, T', \xi')$ is such that $T'(\xi' - d) = \tau_d$ for all $d \in [-1,1]_{\mathbf{Z}}$. Since every configuration locally like C' also satisfies the above condition, it suffices to show that $\langle C'|M_\delta M_\delta^\dagger|C'\rangle$ depends only on $p, \tau_{-1}, \tau_0, \tau_1$. By Proposition 2 and Eq. (7) we have

$$\begin{aligned}
\langle C'|M_\delta M_\delta^\dagger|C'\rangle &= \sum_{C\in\mathcal{C}(Q,\Sigma)} |\langle C'|M_\delta|C\rangle|^2 \\
&= \sum_{C\prec C'} |\langle C'|M_\delta|C\rangle|^2 \\
&= \sum_{q,\sigma,d} |\langle C'|M_\delta|\beta(q,\sigma,d)C'\rangle|^2 \\
&= \sum_{q,\sigma,d} |\langle p, T', \xi'|M_\delta|q, T'^{\sigma}_{\xi'-d}, \xi' - d\rangle|^2 \\
&= \sum_{q,\sigma,d} |\delta(q, T'^{\sigma}_{\xi'-d}(\xi' - d), p, T'(\xi' - d), d)|^2 \\
&= \sum_{q,\sigma,d} |\delta(q,\sigma,p,\tau_d,d)|^2.
\end{aligned}$$

Thus, $\langle C'|M_\delta M_\delta^\dagger|C'\rangle$ depends only on $p, \tau_{-1}, \tau_0, \tau_1$ and the proof is completed. *QED*

For the case where the head is required to move, a proof of the following lemma was sketched first in [8], though with a serious gap, and the corrected proof appeared in [5]. The following proof not only covers the general case but also simplifies the argument given in [5].

Lemma 4. *The evolution operator M_δ of a local transition function δ is unitary if it is isometry.*

Proof. Suppose that M_δ is isometry, i.e., $M_\delta^\dagger M_\delta = 1$. Obviously, $M_\delta M_\delta^\dagger$ is a projection. If $\langle C|M_\delta M_\delta^\dagger|C\rangle = 1$ for every $C \in \mathcal{C}(Q,\Sigma)$, the computational basis is included in the range of $M_\delta M_\delta^\dagger$ and then, since the range of any projection is a closed linear space, we have $M_\delta M_\delta^\dagger = 1$ so that M_δ is unitary. Thus, it suffices to show that $\langle C|M_\delta M_\delta^\dagger|C\rangle = 1$ for every $C \in \mathcal{C}(Q,\Sigma)$. To show this, suppose that there is a configuration $C_0 \in \mathcal{C}(Q,\Sigma)$ such that $\langle C_0|M_\delta M_\delta^\dagger|C_0\rangle = 1 - \varepsilon$ with $\varepsilon > 0$. For any $n > 2$ and $d \in [-1,1]_{\mathbf{Z}}$, let $S(n,d)$ be the set of configurations such that

$$S(n,d) = \{(q,T,\xi) \in \mathcal{C}(Q,\Sigma)|\ T(m) = B \text{ for all } m \notin [1,n]_{\mathbf{Z}} \text{ and } \xi \in [1-d, n+d]_{\mathbf{Z}}\}.$$

Let

$$A = \sum_{(C,C')\in S(n,0)\times S(n,1)} |\langle C'|M_\delta|C\rangle|^2 \tag{8}$$

and we shall consider evaluations of A in terms of the numbers of elements of the sets $S(n,0)$ and $S(n,1)$. It is easy to see that if $C \in S(n,0)$ and $C \prec C'$ then $C' \in S(n,1)$. It follows

from Eq. (7) that $\langle C'|M_\delta|C\rangle = 0$ for any pair (C,C') with $C \in S(n,0)$ and $C' \notin S(n,1)$ so that the summation over $(C,C') \in S(n,0) \times S(n,1)$ in Eq. (8) can be replaced by the summation over $(C,C') \in S(n,0) \times \mathcal{C}(Q,\Sigma)$. By the completeness of the computational basis, we have

$$A = \sum_{(C,C')\in S(n,0)\times\mathcal{C}(Q,\Sigma)} |\langle C'|M_\delta|C\rangle|^2 = \sum_{C\in S(n,0)} \langle C|M_\delta^\dagger M_\delta|C\rangle.$$

Since M_δ is isometry, we have

$$A = |S(n,0)|.$$

Let $S(C_0)$ be the set of all configurations in $S(n,-1)$ locally like C_0. Then, $S(C_0) \subseteq S(n,1)$. By Lemma 3, $\langle C'|M_\delta M_\delta^\dagger|C'\rangle = 1-\varepsilon$ for all $C' \in S(C_0)$. Thus, we have

$$\begin{aligned} A &\le \sum_{(C,C')\in\mathcal{C}(Q,\Sigma)\times S(n,1)} |\langle C'|M_\delta|C\rangle|^2 \\ &= \sum_{C'\in S(n,1)} \langle C'|M_\delta M_\delta^\dagger|C'\rangle \\ &\le (1-\varepsilon)|S(C_0)| + |S(n,1)| - |S(C_0)| \\ &= |S(n,1)| - \varepsilon|S(C_0)|. \end{aligned}$$

The cardinalities of $S(n,d)$ and $S(C_0)$ are given by $|S(n,d)| = (n+2d)|Q|\,|\Sigma|^n$ and $|S(C_0)| = (n-2)|\Sigma|^{n-3}$. Therefore, we have

$$|\Sigma|^{n-3}(2|Q||\Sigma|^3 - \varepsilon(n-2)) = |S(n,1)| - \varepsilon|S(C_0)| - |S(n,0)| \ge 0$$

for all $n > 2$. But, for $n > 2 + 2\varepsilon^{-1}|Q||\Sigma|^3$, this yields an obvious contradiction and the proof is complete. *QED*

According to discussions in Section 3, a quantum Turing machine can be defined as a mathematical structure (Q,Σ,δ) consisting of a Turing frame (Q,Σ) and a local transition function δ such that the evolution operator M_δ is unitary. The following theorem characterizes intrinsically the local transition functions that give rise to quantum Turing machines.

Theorem 5. *The evolution operator M_δ of a local transition function δ for the Turing frame (Q,Σ) is unitary if and only if δ satisfies the following conditions.*

(a) *For any $(q,\sigma) \in Q \times \Sigma$,*

$$\sum_{p,\tau,d} |\delta(q,\sigma,p,\tau,d)|^2 = 1.$$

(b) *For any $(q,\sigma),(q',\sigma') \in Q \times \Sigma$ with $(q,\sigma) \neq (q',\sigma')$,*

$$\sum_{p,\tau,d} \delta(q',\sigma',p,\tau,d)^*\delta(q,\sigma,p,\tau,d) = 0.$$

(c) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q,d=0,1} \delta(q',\sigma',p,\tau',d-1)^*\delta(q,\sigma,p,\tau,d) = 0.$$

(d) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',-1)^*\delta(q,\sigma,p,\tau,1) = 0.$$

Proof. Let δ be a local transition function for a Turing frame (Q,Σ). Let $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$. From Eq. (5) we have

$$\begin{aligned}
&\langle C|M_\delta^\dagger M_\delta|C\rangle \\
&\quad = \sum_{p,\tau,d}\sum_{p',\tau',d'} \delta(q,T(\xi),p',\tau',d')^*\delta(q,T(\xi),p,\tau,d)\langle p',T_\xi^{\tau'},\xi+d'|p,T_\xi^\tau,\xi+d\rangle \\
&\quad = \sum_{p,\tau,d} |\delta(q,T(\xi),p,\tau,d)|^2.
\end{aligned}$$

Since for any $\sigma \in \Sigma$ there is some $T \in \Sigma^\sharp$ and $\xi \in \mathbf{Z}$ such that $T(\xi) = \sigma$, condition (a) holds if and only if $\langle C|M_\delta^\dagger M_\delta|C\rangle = 1$ for any $C \in \mathcal{C}(Q,\Sigma)$.

Let $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$ and $C' = (q',T',\xi') \in \mathcal{C}(Q,\Sigma)$. From Eq. (5) we have

$$\begin{aligned}
&\langle C'|M_\delta^\dagger M_\delta|C\rangle \\
&\quad = \sum_{p,\tau,d}\sum_{p',\tau',d'} \delta(q',T'(\xi'),p',\tau',d')^*\delta(q,T(\xi),p,\tau,d)\langle p',T_{\xi'}^{\tau'},\xi'+d'|p,T_\xi^\tau,\xi+d\rangle \\
&\quad = \sum\nolimits^* \delta(q',T'(\xi'),p,\tau',d')^*\delta(q,T(\xi),p,\tau,d),
\end{aligned}$$

where the summation $\sum^*$ is taken over all $p \in Q$, $\tau,\tau' \in \Sigma$, and $d,d' \in [-1,1]_{\mathbf{Z}}$ such that $T_\xi^\tau = T_{\xi'}^{\tau'}$ and $\xi + d = \xi' + d'$.

For any $k \in \mathbf{Z}$, let $\mathcal{C}(k)$ be a subset of $\mathcal{C}(Q,\Sigma)^2$ consisting of all pairs $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ with $C \neq C'$ such that $T(m) = T'(m)$ for all $m \notin \{\xi,\xi'\}$ and that $\xi' - \xi = k$. It is easy to see that if

$$(C,C') \notin \bigcup_{k\in[-2,2]_{\mathbf{Z}}} \mathcal{C}(k)$$

then $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$. We shall show that condition (b), (c), or (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C,C') \in \mathcal{C}(0)$, $(C,C') \in \mathcal{C}(1)$, or $(C,C') \in \mathcal{C}(2)$, respectively.

For any $(C,C') \in \mathcal{C}(0)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T_{\xi'}^{\prime\tau'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = \tau'$ and $d = d'$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p,\tau,d} \delta(q',T'(\xi'),p,\tau,d)^*\delta(q,T(\xi),p,\tau,d).$$

Since for any $(q,\sigma),(q',\sigma') \in Q\times\Sigma$ with $(q,\sigma) \neq (q',\sigma')$ there are configurations $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ such that $(C,C') \in \mathcal{C}(0)$, $T(\xi) = \sigma$ and $T'(\xi') = \sigma'$, condition (b) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for all $(C,C') \in \mathcal{C}(0)$.

For any $(C,C') \in \mathcal{C}(1)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T_{\xi'}'^{\tau'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = T'(\xi)$, $\tau' = T(\xi')$, and $(d,d') \in \{(0,-1),(1,0)\}$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p\in Q,d=0,1} \delta(q',T'(\xi'),p,T(\xi'),d-1)^*\delta(q,T(\xi),p,T'(\xi),d).$$

Since for any $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$ there are configurations $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ such that $C,C' \in \mathcal{C}(1)$, $(T(\xi),T'(\xi)) = (\sigma,\tau)$, and $(T'(\xi'),T(\xi')) = (\sigma',\tau')$, condition (c) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for any $(C,C') \in \mathcal{C}(1)$.

For any $(C,C') \in \mathcal{C}(2)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T_{\xi'}'^{\tau'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = T'(\xi)$, $\tau' = T(\xi')$, $d = 1$, and $d' = -1$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p\in Q} \delta(q',T'(\xi'),p,T(\xi'),-1)^*\delta(q,T(\xi),p,T'(\xi),1).$$

Thus, condition (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for all $(C,C') \in \mathcal{C}(2)$.

Since $M_\delta^\dagger M_\delta$ is self-adjoint, M_δ is isometry if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = \boldsymbol{\delta}_C^{C'}$ for any $C = (q,T,\xi)$, $C' = (q',T',\xi') \in \mathcal{C}(Q,\Sigma)$ with $\xi \leq \xi'$. Therefore, we have proved that conditions (a)–(d) hold if and only if M_δ is isometry. Now, Lemma 4 concludes the assertion. *QED*

5. Multi-tape Quantum Turing machines

In the preceding sections, we have discussed solely single tape quantum Turing machines, but our arguments can be adapted easily to multi-tape quantum Turing machines, which are quantum analogues of multi-tape deterministic Turing machines.

For example, a two-tape quantum Turing machine is a quantum system consisting of a processor, two bilateral infinite tapes with heads to read and write symbols on their tapes. In order to discuss local transition functions, we adapt the formal definitions as follows. Let (Q,Σ_1,Σ_2) be a triple, called a *two-tape Turing frame*, consisting of a finite sets Q, Σ_1, and Σ_2 with specific elements $B_1 \in \Sigma_1$ and $B_2 \in \Sigma_2$. The *configuration space* of (Q,Σ_1,Σ_2) is the product set $\mathcal{C}(Q,\Sigma_1,\Sigma_2) = Q\times\Sigma_1^\#\times\Sigma_2^\#\times\mathbf{Z}^2$. Thus, the configuration of a two-tape quantum Turing machine $\mathcal{Q}$ with the frame (Q,Σ_1,Σ_2) is determined by the processor configuration $q \in Q$, the first and second tape configurations $T_1 \in \Sigma_1^\#$, $T_2 \in \Sigma_2^\#$, and the head positions $\xi_1 \in \mathbf{Z}$, $\xi_2 \in \mathbf{Z}$ in the first and second tapes. The *quantum state space* of (Q,Σ_1,Σ_2) is the Hilbert space $\mathcal{H}(Q,\Sigma_1,\Sigma_2)$ generated by $\mathcal{C}(Q,\Sigma_1,\Sigma_2)$. A *local transition function* for (Q,Σ_1,Σ_2) is defined to be a complex-valued function on $Q\times\Sigma\times Q\times\Sigma\times[-1,1]_{\mathbf{Z}}^2$, where $\Sigma = \Sigma_1\times\Sigma_2$. The relation $\delta(q,(\sigma_1,\sigma_2),p,(\tau_1,\tau_2),(d_1,d_2)) = c$ can be interpreted as the

following operation of $\mathcal{Q}$: if the processor is in the configuration q and if the head of the i-th tape ($i = 1, 2$) reads the symbol σ_i, then it follows with the amplitude c that the processor configuration turns to p, the head of the i-th tape writes the symbol τ_i and moves one cell to the right if $d_i = 1$, to the left if $d_i = -1$, or does not move if $d_i = 0$. The *evolution operator* of δ is a linear operator M_δ on $\mathcal{H}(Q, \Sigma_1, \Sigma_2)$ such that

$$M_\delta|q, (T_1, T_2), (\xi_1, \xi_2)\rangle$$
$$= \sum \delta(q, (T_1(\xi_1), T_2(\xi_2)), p, (\tau_1, \tau_2), (d_1, d_2))|p, (T_{1\xi_1}^{\tau_1}, T_{2\xi_2}^{\tau_2}), (\xi_1 + d_1, \xi_2 + d_2)\rangle$$

for all $(q, (T_1, T_2), (\xi_1, \xi_2)) \in \mathcal{C}(Q, \Sigma_1, \Sigma_2)$, where the summation is taken over all $(p, (\tau_1, \tau_2), (d_1, d_2)) \in Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}^2$. Then, local transition functions of two-tape quantum Turing machines are characterized as follows.

Theorem 6. *The evolution operator M_δ of a local transition function δ for the two-tape Turing frame (Q, Σ_1, Σ_2) is unitary if and only if δ satisfies the following conditions.*

(1) *For any $(q, \sigma) \in Q \times \Sigma$,*

$$\sum_{p \in Q, \tau \in \Sigma, d_1, d_2 \in [-1,1]_{\mathbf{Z}}} |\delta(q, \sigma, p, \tau, (d_1, d_2))|^2 = 1.$$

(2) *For any $(q, \sigma), (q', \sigma') \in Q \times \Sigma$ with $(q, \sigma) \neq (q', \sigma')$,*

$$\sum_{p \in Q, \tau \in \Sigma, d_1, d_2 \in [-1,1]_{\mathbf{Z}}} \delta(q', \sigma', p, \tau, (d_1, d_2))^* \delta(q, \sigma, p, \tau, (d_1, d_2)) = 0.$$

(3) *For any $(q, \sigma, \tau_2), (q', \sigma', \tau_2') \in Q \times \Sigma \times \Sigma_2$,*

$$\sum_{\substack{p \in Q, \tau_1 \in \Sigma_1 \\ d_1 \in [-1,1]_{\mathbf{Z}}, d_2 = 0,1}} \delta(q', \sigma', p, (\tau_1, \tau_2'), (d_1, d_2 - 1))^* \delta(q, \sigma, p, (\tau_1, \tau_2), (d_1, d_2)) = 0.$$

(4) *For any $(q, \sigma, \tau_2), (q', \sigma', \tau_2') \in Q \times \Sigma \times \Sigma_2$,*

$$\sum_{p \in Q, \tau_1 \in \Sigma_1, d_1 \in [-1,1]_{\mathbf{Z}}} \delta(q', \sigma', p, (\tau_1, \tau_2'), (d_1, -1))^* \delta(q, \sigma, p, (\tau_1, \tau_2'), (d_1, 1)) = 0.$$

(5) *For any $(q, \sigma, \tau), (q', \sigma', \tau') \in Q \times \Sigma^2$,*

$$\sum_{p \in Q, d_1 = 0,1} \delta(q', \sigma', p, \tau', (d_1 - 1, 1))^* \delta(q, \sigma, p, \tau, (d_1, -1)) = 0.$$

(6) *For any $(q, \sigma, \tau), (q', \sigma', \tau') \in Q \times \Sigma^2$,*

$$\sum_{p \in Q, d_1 = 0,1, d_2 = 0,1} \delta(q', \sigma', p, \tau', (d_1 - 1, d_2))^* \delta(q, \sigma, p, \tau, (d_1, d_2 - 1)) = 0.$$

(7) *For any* $(q,\sigma,\tau_1),(q',\sigma',\tau_1') \in Q\times\Sigma\times\Sigma_1$,

$$\sum_{\substack{p\in Q,\tau_1\in\Sigma_1\\ d_1=0,1,d_2\in[-1,1]_{\mathbf{Z}}}} \delta(q',\sigma',p,(\tau_1',\tau_2),(d_1-1,d_2))^*\delta(q,\sigma,p,(\tau_1,\tau_2),(d_1,d_2))=0.$$

(8) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1,d_2=0,1} \delta(q',\sigma',p,\tau',(d_1-1,d_2-1))^*\delta(q,\sigma,p,\tau,(d_1,d_2))=0.$$

(9) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1} \delta(q',\sigma',p,\tau',(d_1-1,-1))^*\delta(q,\sigma,p,\tau,(d_1,1))=0.$$

(10) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',(-1,1))^*\delta(q,\sigma,p,\tau,(1,-1))=0.$$

(11) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_2=0,1} \delta(q',\sigma',p,\tau',(-1,d_2))^*\delta(q,\sigma,p,\tau,(1,d_2-1))=0.$$

(12) *For any* $(q,\sigma,\tau_1),(q',\sigma',\tau_1') \in Q\times\Sigma\times\Sigma_1$,

$$\sum_{p\in Q,\tau_2\in\Sigma_2,d_2\in[-1,1]_{\mathbf{Z}}} \delta(q',\sigma',p,(\tau_1',\tau_2),(-1,d_2))^*\delta(q,\sigma,p,(\tau_1,\tau_2),(1,d_2))=0.$$

(13) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_2=0,1} \delta(q',\sigma',p,\tau',(-1,d_2-1))^*\delta(q,\sigma,p,\tau,(1,d_2))=0.$$

(14) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$,

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',(-1,-1))^*\delta(q,\sigma,p,\tau,(1,1))=0.$$

If each head is required to move either to the right or to the left at each step, conditions (3),(5)–(9),(11), and (13) are automatically satisfied. It is also easy to see that conditions (3)–(14) are automatically satisfied by unidirectional two-tape quantum Turing machines, for which (d_1,d_2) is uniquely determined by p in the non-zero amplitude $\delta(q,\sigma,p,\tau,(d_1,d_2))$ [5].

The proof of Theorem 6 is analogous to the proof of Theorem 5. Let $\mathcal{C}(k_1, k_2)$ be a subset of $\mathcal{C}(Q, \Sigma_1, \Sigma_2)^2$ consisting of all pairs $C = (q, (T_1, T_2), (\xi_1, \xi_2))$ and $C' = (q', (T_1', T_2'), (\xi_1', \xi_2'))$ with $C \neq C'$ such that $T_i(m_i) = T_i'(m_i)$ for $m_i \notin \{\xi_i, \xi_i'\}$ and that $\xi_i' - \xi_i = k_i$ for $i = 1, 2$. This plays a role similar to $\mathcal{C}(k)$ in the proof of Theorem 5. In the proof of Theorem 5, we showed that condition (b),(c), or (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C, C') \in \mathcal{C}(0), (C, C') \in \mathcal{C}(1)$, or $(C, C') \in \mathcal{C}(2)$, respectively. In the case of Theorem 6, we can show similarly that for $k_1 \in [0, 2]_{\mathbf{Z}}$ and $k_2 \in [-2, 2]_{\mathbf{Z}}$, condition $(5k_1 + k_2 + 2)$ holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C, C') \in \mathcal{C}(k_1, k_2)$. Moreover, it is trivial that condition (1) holds if and only if $\langle C|M_\delta^\dagger M_\delta|C\rangle = 1$ holds for all $C \in \mathcal{C}(Q, \Sigma_1, \Sigma_2)$, and that if

$$(C, C') \notin \bigcup_{(k_1,k_2)\in[-2,2]_{\mathbf{Z}}^2} \mathcal{C}(k_1, k_2)$$

then $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$. Since $M_\delta^\dagger M_\delta$ is self-adjoint, M_δ is isometry if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = \delta_C^{C'}$ for any $C = (q, (T_1, T_2), (\xi_1, \xi_2)), C' = (q, (T_1', T_2'), (\xi_1', \xi_2')) \in \mathcal{C}(Q, \Sigma_1, \Sigma_2)$ with $\xi_1 < \xi_1'$ or with $\xi_1 = \xi_1'$ and $\xi_2 \leq \xi_2'$. Therefore, we can show that conditions (1)–(14) hold if and only if M_δ is isometry. We can also show that M_δ is unitary if it is isometry by a similar argument with the proof of Lemma 4. Thus we can prove Theorem 6. Similarly, local transition functions of k-tape quantum Turing machines can be characterized by $1 + (1/2)(5^k + 1)$ conditions in general.

Multi-tape Turing machines are often used for theoretical considerations in complexity theory [10] because it is often easier to construct a multi-tape machine than a single tape machine in order to realize a given algorithm. Hence, multi-tape quantum Turing machines can be expected as useful tools for quantum complexity theory. In such applications, it appears to be a tedious task to check that a constructed local transition function satisfies the unitarity conditions. However, restricted classes of multi-tape machines are characterized much more simply; the two-way two-tape machines are characterized by 6 conditions out of 14 and the unidirectional multi-tape machines are characterized by only two conditions such as conditions (1) and (2) in Theorem 6.

In [9], we generalized Yao's construction [6] of quantum circuits simulating single tape quantum Turing machine to multi-tape quantum Turing machines and also showed that any uniform quantum circuit family can be simulated by a single tape unidirectional quantum Turing machine. Thus, the class of multi-tape quantum Turing machines is computationally equivalent with the single tape quantum Turing machines.

References

[1] R. P. Feynman, *Simulating physics with computers*, Internat. J. Theoret. Phys., 21 (1982), pp. 467–488.

[2] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. London Ser. A, 400 (1985), pp. 97–117.

[3] D. Deutsch, *Quantum computational networks*, Proc. Roy. Soc. London Ser. A, 425 (1989), pp. 73–90.

[4] P. Benioff, *The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines*, J. Stat. Phys., 22 (1980), pp. 563–591.

[5] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM J. Comput., 26 (1997), pp. 1411–1473.

[6] A. Yao, *Quantum circuit complexity*, in Proc. 34th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1993, pp. 352–361.

[7] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1994, pp. 124–134,.

[8] E. Bernstein and U. Vazirani, *Quantum complexity theory (Preliminary abstract)*, in Proc. 25th Annual ACM Symposium on Theory of Computation, ACM Press, New York, 1993, pp. 11–20.

[9] H. Nishimura and M. Ozawa, *Computational complexity of uniform quantum circuit families and quantum Turing machines*, (in preparation).

[10] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley, Reading, MA, 1994.